بسم الله الرحمن الرحيم

الفايروسات ومكافحتها

محمد اسماعيل محمد

فيروس الحاسوب

فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب و ما شابهها من عمليات. اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه،وتتم كتابتها بطريقة معينة.

- نبذة تاريخية:

بدأ ظهور أول فيروس سنة 1978م أو قبلها بقليل (بحيث يصعب تحديد البداية بدقة) ولم تأخذ المشكلة شكلها الحالي من الخطورة إلّا مع انتشار استخدام شبكة الانترنت ووسائل الاتصالات المعقدة، منها: البريد الإلكتروني.

حيث أمكن ما لم يكن ممكناً من قبل من ناحية مدى انتشار الفيروس ومدى سرعة انتشاره.

- لماذا سمي الفيروس بهذا الاسم؟

تطلق كلمة فيروس على الكائنات الدقيقة التي تنقل الأمراض للإنسان وتنتشر بسرعة مرعبة. وبمجرد دخولها إلى جسم الإنسان تتكاثر وتفرز سمومها حتى تسبب دمار الأجهزة العضوية للجسم ومنها ما هو قاتل يسبب الموت.

والفيروس عندما يدخل إلى الكمبيوتر يعمل نفس التأثيرات ونفس الأفعال، وله نفس قدرة التكاثر وربط نفسه بالبرامج حتى يسبب دمار الكمبيوتر دماراً شاملاً.

وهناك بعض أوجه الشبه بين الفيروس الحيوي والفيروس الإلكتروني منها:

1- يقوم الفيروس العضوي بتغيير خصائص ووظائف بعض خلايا الجسم .. وكذلك الفيروس الالكتروني يقوم بتغيير خصائص ووظائف البرامج والملفات.

2- يتكاثر الفيروس العضوي ويقوم بإنتاج فيروسات جديدة .. كذلك الفيروس الإلكتروني يقوم بإعادة إنشاء نفسه منتجاً كميات جديدة.

3- الخلية التي تصاب بالفيروس لا تصاب به مره أخرى (سنحتاج هذه المعلومة لاحقا) أي يتكون لديها مناعة .. وكذلك الحال مع الفيروس الإلكتروني حيث أنه يختبر البرامج المطلوب إصابتها فإن كانت أصيبت من قبل لا يرجع إليها بل ينتقل إلى برامج أخرى وملفات جديدة.

4- الجسم المصاب بالفيروس قد يظل مدة بدون ظهور أي أعراض (فتره الحضانة) .. وكذلك البرامج المصابة قد تظل تعمل مدة طويلة بدون ظهور أي أعراض عليها.

5- يقوم الفيروس العضوي بتغيير نفسه حتى يصعب اكتشافه (الإيدز مثلاً) .. وكذلك الفيروس الإلكتروني فإنه يتشبه بالبرامج حتى لا يقوم أي مضاد للفيروسات باكتشافه.

ومن خلال هذه الأسباب يتضح لماذا سمي الفيروس بهذا الاسم رغم أنه في الواقع ليس سوى برنامج من برامج الكمبيوتر. وقد كان التشابه بين الفيروسين سبباً لبعض المواقف الطريفة.. منها أن بعض الناس أصابه الرعب لدرجة أنهم يتناقلون الأقراص وهم يرتدون القفازات وكأنه فيروس حيوي ينتقل في الجو!

أسباب التسمية

سمي الفيروس (Virus) بهذا الاسم لتشابه آلية عمله مع تلك التي تصيب الكائنات الحية بعدد من الخصائص، كخاصية الانتقال بالعدوى، أو كونه كائنا غريبا يقوم بتغيير حالة الكائن المصاب، إضافة إلى الضرر الذي يعقبه إن لم يتم العلاج. سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين: اولا : تحتاج فيروسات الكومبيوتر دائماً إلى ملف عائل تعيش متستّرةً فيه. فالفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفايروس ايضا تشبه بطريقه هذه الفيروسات البيولوجيه حيث لا يستطيع اي فايروس العيش بدون اصابته لخليه في جسم الكائن الحي (بدون الخليه يتلف الفايروس ويتلاشى) . ثانيا : انتقالها يشبه طريقة انتقال الفيروسات البيولوجيه حيث تتواجد الفايروسات في مكان اساسي في

الحاسب كالذاكره رام مثلا وتصيب اي ملف يشغل في اثناء وجودها بالذاكره مما يزيد عدد الملفات المصابه كلما طال وقت اكتشاف الفايروس (كما الفايروس البيولوجي بعد استنزافه للخليه الحية يدمرها ويتكاثر في خلايا اخرى .

أعراض الإصابة

- تكرار رسائل الخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع نظام التشغيل أو تنفيذ بعض التطبيقات.

رفض بعض التطبيقات للتنفيذ.

فالفيروس، عبارة عن برنامج صمم لينشر نفسه بين الملفات ويندمج أو يلتصق بالبرامج. فعند تشغيل البرنامج المصاب فإنه قد يصيب باقي الملفات الموجودة معه في القرص الصلب أو المرن، لذا يحتاج الفيروس إلى تدخل من جانب المستخدم كي ينتشر، بطبيعة الحال التدخل عبارة عن تشغيله بعد أن تم جلبه من الايميل أو تنزيله من الانترنت أو من خلال تبادل الاقراص المرنة.

تعمل الفيروسات بطبيعتها على تعطيل عمل الحاسوب أو تدمير ملفاته وبرامجة وهناك أنواع مزعجة بعض الشي تعمل حسب ميكانيكية معينة فعلى سبيل المثال هناك فيروسات تعمل على خلق رسائل مزعجة في أوقات متفرقة وهناك أنواع تعمل على تشغيل برامج غير مطلوبة وهناك أنواع تعمل على اشغال المعالج بحيث تبطئ سرعة الحاسوب.

أنواع الفيروسات

أنواع الفيروسات ثلاثة الفيروس والدودة وحصان طروادة ما الفرق بين الفيروس والدودة وحصان طروادة

• الفيروس: يمكن القول بأنه برنامج تنفيذي يعمل بشكل منفصل ويهدف إلى احداث خلل في نظام الحاسوب وتتراوح خطورته حسب مهمته فمنه الخبيث ومنه الحميد وكلاهما خبيث.

• الدودة (worm): فيروس ينتشر فقط عبر الشبكات والانترنت ويعمل على الانتشار على الشبكات عن طريق دفتر عناوين البريد الالكتروني مثلا فعند اصابة الجهاز يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في دفتر العناوين على سبيل المثال ويرسل نفسه إلى كل شخص وهكذا ... مما يؤدي إلى انتشاره بسرعه عبر الشبكه وقد اختلف الخبراء فمنهم اعتبره فايروس ومنهم من اعتبره برنامج خبيث وذلك كون الدوده لاتنفذ اي عمل مؤذي انما تنتشر فقط مما يؤدي إلى اشغال موارد الشبكه بشكل كبير ومع التطور الحاصل في ميدان الحوسبه اصبح بامكان المبرمجين الخبيثين اضافة سطر برمجي لملف الدوده بحيث تؤدي عمل معين بعد انتشارها (مثلا بعد الانتشار إلى عدد 50000 جهاز يتم تخريب الانظمة في هذه الاجهزة) او اي شئ اخر (مثلا في يوم معين او ساعة او تاريخ ...الخ) واصبحت الديدان من أشهر الفيروسات على الشبكه العالميه واشهر عملياتها التخريبيه واخطرها تلك التي يكون هدفها حجب الخدمه تسمى (هجمات حجب الخدمه) حيث تنتشر الدوده على عدد كبير من الاجهزة ثم توجه طلبات وهميه لجاهز خادم معين (يكون المبرمج قد حدد الخادم المستهدف من خلال برمجته للدوده) فيغرق الخادم بكثرة الطلبات الوهميه ولا يستطيع معالجتها جميعا مما يسبب توقفه عن

العمل وهذه الديدان استهدفت مواقع لكثير من الشركات العالمية اشهرها مايكروسوفت وغيرها الكثير .

- حصان طروادة Trojan Horse: سمي هذا الفيروس بحصان طروادة لانه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون الية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج مادون ان يعلم المستخدم. فعندما يبدأ البرنامج تنفيذ عمله ويصل إلى مرحلة ما الفيروس يبدأ العمل والتخريب وقد لا يكون هدف الفايروس التخريب هنا قد يكون هدفه ربحي كما حصل في احدى المدن الانكليزيه حيث تم توزيع قرص مجاني على المشافي به برنامج حول مرض الايدز (اسبابه - طرق انتشاره - طرق العلاج .. الخ) وبعد مدة شهر من تشغيل البرنامج تم تشفير المعلومات على الحواسب الحاضنه للفايروس وظهرت رساله مفادها ان الحاسب مصاب بالايدز (المقصود هنا انه تم تشفير ملفات الحاسب وايقافها عن العمل بطريقه نظاميه) ارسل مبلغ كذا إلى الحساب كذا ليتم ارسال رقم فك الشيفره مما اجبر المختصين بالرضوخ للطلب كونهم لم يستطيعو فك التشفير . توجد عدة تقسيمات للفيروسات، فمثلاً من حيث سرعة الانتشار هناك فيروسات سريعة الانتشار وفيروسات بطيئة الانتشار ومن حيث توقيت النشاط فيروسات تنشط في أوقات محددة وفيروسات دائمة النشاط ومن حيث مكان الإصابة فيروسات مقطع التشغيل boot sector على الأقراص وهي الأكثر شيوعاً، وفيروسات الماكرو macro التي تختص بإصابة الوثائق والبيانات الناتجة عن حزمة مايكروسوفت أوفيس، أما من حيث حجم الضرر فهناك الفيروسات المدمرة للاجهزة طبعا لايوجد فايروسات خارقه بحيث انها تدمر الاجهزة كما نسمع احيانا (احترق المعالج بسبب الفايروس تعطلت وحدة

التغذيه بسبب الفايروس او تلفت الشاشة بسبب الفايروس ،... الخ) ولكن يمكن للفايروس ان يؤذي الذاكره روم في الحاسب كما في فايروس تشرنوبل او ان يمحي معلومات ال MBR على القرص الصلب فتعود الاقراص الصلبه كما اتت من المصنع وفي الحالتين السابقتين لا يتم اقلاع الجهاز مما يوحي للبعض ان الفايروس (حرق) الحاسب طبعا هذه الفيروسات تعتبر خطيره جدا لانها تتسبب في اتلاف البيانات المخزنه والتي قد تكون (البيانات) نتاج عشرات السنين مما يؤديي إلى خسائر جسيمة او إلى توقف الحاسبات عن العمل كما في تشرنوبل مما يؤدي إلى توقف الخدمات المقدمه ، وهنالك ايضا والفيروسات المدمرة للبرامج وتاثيرها محدود طالما ان البيانات لم تتاثر حيث يمكن تخزين البيانات واعادة تهئية الحاسب واعادة البرامج المتضرره من اقراصها الاصليه، والفيروسات عديمة الضرر وهي التي لاتقوم باي عمل مؤذي وانما تم برمجتها لاثبات الذات والقدره على البرمجه من بعض المراهقين فمنها ما يرسم كره على الشاشه طوال فترة عمل الكمبيوتر ومنها ما يغير بعض الاحرف (كتغير حرف بحرف اينما وجد) او تغيير مؤشر الماوس .. الخ.

لماذا يخلق الناس فيروسات الحاسوب

فيروسات الحاسوب لا تتشابه في وجودها بالفيروسات الحيوية. إن فيروس الحاسوب لا ينشئ من لا شيء أو لا ياتي من مصدر مجهول أو لا ينشئ بسبب خلل بسيط حدث في الحاسوب. فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمة بشكل متقن. يعمل المبرمجون على خلق الفيروسات وذلك لاهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين يعتبرون أن عمل الفيروس نوع

من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات. يذكر أن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

أغلب برامج التجسس الشخصية تتكون عادة من ملفين الأول هو ما يسمى بالريموت وهذا هو الملف الذي يتحكم به المخترق في جهازك وينزل عن طريق هذه الأداة المعلومات التي يريد من نظامك

والملف الثاني هو ما يسمى بالخادم وله عدة أسماء ثانية مثل السيرفر server أو الباتش batch وهذا الملف لابد من من أن تقوم بتشغيله في جهازك لكي يستطيع المخترق أن يدخل جهازك

كل برنامج من برامج التجسس يستخدم سيرفر خاص به يدعم خصائصه وعادة ما يتراوح حجم السيرفر من 100 كيلوبايت الى 400 كيلوبايت والحجم يعتمد على كمية الخصائص الموجودة بالريموت

والحجم لا أساس له فقد يقوم المخترق بدمج ملف السيرفر مع برنامج آخر أو لعبة صغيرة لتقوم أنت بتشغيلها وفي كل مرة تقوم بتشغيل اللعبة أو البرنامج فأن السيرفر المدمج بها يقوم بتشغيل نفسه أوتوماتيكياً

ولرؤية قائمة بالبرامج التي تعمل على دمج السيرفر أو الفيروس بأي ملف او برنامج اذهب للموقع التالي

http://paragon.revoluti0n.org/dlbind.htm

وملف السيرفر يقوم بفتح منفذ لديك بجهازك ليستقبل عن طريقه الأوامر المرسلة اليه من المخترق عن طريق أداة الريموت ويرد عليه بالمعلومات المطلوبة عن طريق نفس المنفذ والمنفذ الذي يستخدمه السيرفر يختلف من برنامج أختراق لآخر وبعض البرامج تقوم بتخييرك لأي منفذ تريد الأختراق عبره وبمجال معين لكل برنامج

ولرؤية قائمة بالمنافذ الأفتراضية لبرامج الأختراق الشهيرة اذهب للموقع التالي :

http://paragon.revoluti0n.org/Text/trojanports.txt

والسيرفر عادة يعمل تلقائيا في كل مرة تقوم فيها بتشغيل الويندوز لديك ولا يمكنك التخلص منه بأعادة تشغيل جهازك فقط

وهنالك عدة برامج تعمل على تنظيف جهازك من الباتشات وأشهرها هو الكلينر أو المنظف ويمكنك الحصول عليه من موقع كويت كيس http://www.qkiss.com ولكن هذه البرامج غير عملية فقد يعمل المخترق على تغيير الكود الخاص بالسيرفر بحيث لا تكتشفه برامج الأختراق ومن الممكن أن يغير رقم المنفذ الذي يتعامل مع السيرفر عن طريقه وأفضل طريقة لأبقاء جهازك بعيدا عن أيدي المخترقين هي تنظيفه بنفسك ولقد حاولت هنا قدر الأمكان جمع المعلومات عن طرق عمل سيرفرات الأختراق وكيفية أزالتها من جهازك بالطريقة السليمة وبنفسك

الباك دور BackDoor :

وهو أيضا يحتاج إلى خادم لتشغيله. ويوجد إصدارين من هذا البرنامج.

للتخلص من الإصدار الأول قم مباشرة بإلغاء الملفات التالية إذا كانت موجودة على جهازك :

TINURAK.EXE WATCHING.DLL DATA2.EXE

وللتخلص من الإصدار الثاني قم مباشرة بإلغاء الملفات التالية إذا كانت موجودة على جهازك :

NODLL.EXE SERVER_33.DLL WINDOW.EXE

الباك اورفيس :

برنامج الباك أورفيس يعمل على الويندوز 95 والويندوز 98 فقط وحجم السيرفر الخاص به صغير نسبيا - تقريباً 120 كيلوبايت فقط

والمنفذ الذي يستخدمه الباك اورفيس هو 31337 فقط

والتخلص منه يكون بالخطوات التالية :

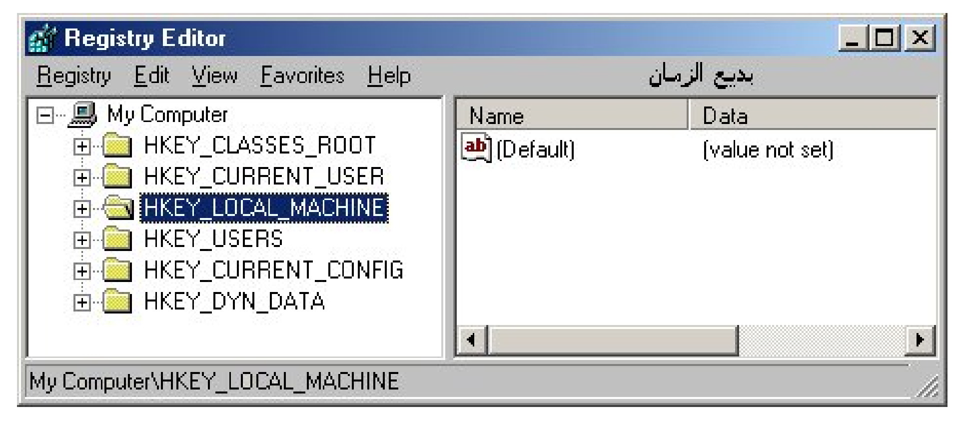
قم بتشغيل محرر التسجيل عن طريق أبدأ ثم تشغيل ثم أكتب Regedit (شكل 1)



ثم قم بالذهاب الى المفتاح التالي :

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRunService

(شكل 2)



قم بالبحث في القائمة اليمنى عن أي ملف يثير الشبهة لديك وأنقر عليه نقرتين لتجد مكان الملف في جهازك وتأكد من أن حجمه حوالى 120 كيلوبايت فأذا وجدته قم بمسحه وأعادة تشغيل جهازك

ثم أذهب للمجلد التالي

C:WindowsSystem

وقم بالبحث هناك عن أسم السيرفر وسيكون بنفس الأسم الذي وجدته في محرر التسجيل وقم بحذفه تماما من الجهاز وستجد ملفاً آخرا أسمه

Windll.dll

قم بحذفه هو أيضا لأنه تابع لباك أورفيس

بعد حذفك للملفات قم بأيقاف تشغيل جهازك نهائيا وفصله من الكهرباء أيضا

الباك اورفيس BO2k 2000:

وهو يتمكن من وندوز 95 و وندوز 98 و وندوز إن تي ، ولهذا البرنامج نسختين الأولى تسمى النسخة الأمريكية وهي أكبر حجما من النسخة الأخرى بالكيلو بايت طبعا. أيضا لهذه النسخة ميزة أخرى تعرف بـ DES encryption أما النسخة الثانية فتسمى النسخة الدولية

الأسماء المستعارة لهذا البرنامج التي يتخفى بها هي :

backdoor.BO2K BO2K

طريقة معرفة وجودة في جهازك والتخلص منه :

يوجد الآن برنامج واحد لحمايتك من هذا البرنامج تجده في الموقع التالي

http://www.spiritone.com/~cbenson/current_projects/backorifice/backorifice.htm

----

النت بس NetBus 1.x :

ويستخدم خادم داخل جهازك ومتمكن أيضا من وندوز 95 و 98 و إن تي ويستطيع عمل كل شي يعمله برنامج السب سفن إضافة إلى انه يستطيع إن يتحكم بالفارة التي لديك ويمكنه عرض بعض الصور على شاشة جهازك أيضا أن يفتح محرك أقراص الليزر الخاص بك أيضا باستطاعته سماع كل شي تقوله إذا كنت موصل مايكروفون مع جهازك وأشياء أخرى عديدة حجم السيرفر الخاص به هو 470 كيلو بايت ، ويمكن لصاحبه الدخول اليك من المنفذ 12345 والمنفذ 12346

طريقة التخلص منه كالتالي :

قم بتشغيل محرر التسجيل وذلك بالطريقة التالية

أبدا - تشغيل - ثم أكتب في المربع الأمر التالي

Regedit (كما في شكل 1)

ثم أذهب إلى المفتاح التالي

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun

ستجد هنالك قائمة بالبرامج التي تعمل بجهازك مع بدء التشغيل فقط قم بحذف أي ملف تشك بأنه هو السيرفر لأن السيرفر لا اسم محدد له وقد يكون بأي اسم

من ثم أذهب إلى المجلد التالي

c:WindowsSystem

وستجد هنالك ملف بنفس اسم القيمة التي قمت بمسحها فقط قم بمسح هذا الملف وإذا رفض الملف المسح –وعادة ما سيرفض ذلك لأنه يعمل في نفس الوقت الذي تحاول مسحه – فقم بتشغيل الويندوز في الوضع الآمن وامسحه أو قم بمسحه من الدوس وتأكد من أنك مسحت السيرفر وليس ملف آخر ويمكنك التأكد عن طريق الحجم الذي يتراوح ما بين 400 كيلوبايت و 500 كيلوبايت فقط

ثم قم بأعادة تشغيل جهازك وستجد أن السيرفر قد تم أزالته عند مراجعتك للخطوات السابقة

السب سيفن Sub7 :

برنامج السب سفن هو من أشهر برامج الأختراق وأكثرها قدرة على التحكم في جهاز الضحية ولهذا فالسيرفر الخاص به خطير جدا ولابد من التأكد من عدم وجوده بجهازك

يقوم السيرفر الخاص بالسب سفن بوضع الملفات التالية في مجلد الويندوز الخاص بك

Kernel.dl

Rundll16.exe

Movokh_32.dll

Watching.dll

Nodll.exe

مع العلم أنه يمكن تغيير أسماء الملفات السابقة من قبل المخترق

كما يقوم بأنشاء القيم التالية في سجل الويندوز لديك:

HKEY_LOCAL_MACHINESoftwareCLASSES.dl
HKEY_LOCAL_MACHINESoftwareMicrosoftDirectXMediaKER

"NEL16="KERNEL16.DL

HKEY_LOCAL_MACHINESoftwareCLASSES.dl@=exefile

أيضا يقوم السيرفر بأضافة أوامر للملفات التالية

Shell=Explorer.exe rundll16.exe<=== System.ini

Run=????.exe Or Load=????.exe <==== Win.ini

والمنافذ التي يقوم بأختراق جهازك عن طريقها هي 6711 و 6776 أو أي رقم يتراوح ما بين 1243 و 1999 وذلك بحسب رغبة المخترق

وطريقة التخلص منه كالتالي:

قم بالذهاب الى الملفين

System.ini

Win.ini

عن طريق الخطوات : أبدأ – تشغيل – ثم أكتب في مربع التشغيل

msconfig



بالنسبة لملف الوين فقط قم بالبحث عن الأوامر التالية :

Load=???.exe

Load=???.dll

Run=???.exe

وعلامات الأستفهام ترمز الى اسم السيرفر وقد تكون أي شئ

ثم أذهب الى الملف النظام وفي السطر الخامس تقريبا ستجد شيئاً كالتالي

Shell=Explorer.exe

وأذا وجدت السطر مكتوبا بطريقة غير السابق قم بتعديله ليصبح كالسابق

وقد يكون هكذا اسمه

Shell=Explorer.exe ???.dll

وعلامات الأستفهام ترمز لأسم السيرفر فقط قم أنت بتعديل السطر الى

Shell=Explorer.exe

بعد ذلك أذهب الى محرر التسجيل عن طريق الخطوات

أبدا ثم تشغيل ثم أكتب في مربع النص التالي

Regedit

وأذهب الى المفتاح التالي

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun

وستجد على القائمة اليمنى أسم السيرفر وستعرفه بالطبع لأنه سيكون بنفس الأسم الذي وجدته سابقاً في ملف النظام فقط قم بمسح القيم التي ترمز الى السيرفر بالنقر على زر الحذف

والآن قم بأعادة تشغيل جهازك وأذهب الى مجلد الويندوز وقم بحذف السيرفر وسيكون اسمه معروفا لك الآن

The FreeLinl :

وهو يعتبر دودة مشفرة يعمل تحت أي وندوز تدعم لغة

VB scripting

حتى وندوز 98 و وندوز 2000 ومعظم طرق دخوله إلى جهازك عن طريق البريد الألكتروني ويكون عنوان المرسل كالتالي هو

Check this

وتكون الرسالة المصاحبة لهذا العنوان هي :

these links. Bye Have fun with

فإذا قمت بالدخول علية فأنة يقوم مباشرة بتحميل ملفين على جهازك هما :

c:windowslinks.vbs c:windowssystemrundll.vbs

أيضا يضيف الجزء التالي إلى جهازك في سجل الويندوز

HKEY_LOCAL_MACHINESoftwaremicrosoftwindowsCurrentVersionRunRundll

RUNDLL.VBS=

وبعد التمكن من جهازك سوف يعرض على الشاشة صندوق صغير بالعنوان التالي

links Free XXX

وتحت العنوان تظهر الرسالة التالية:

a shortcut to free XXX links on your desktop This will add ?Do you want to continue

ثم سوف يقوم هذا البرنامج بالبحث عن برامج المحادثة مثلmirc

Pirch98.exe MIRC32.exe

وسوف يقوم بتعديل الملفات التالية :

EVENTS.INI SCRIPT.INI

وذلك حتى يتمكن من إرسال

LINKS.VBS

إلى أجهزة أخرى أثناء عملية المحادثات بين المستخدمين

والأسماء المستعارة لهذا البرنامج التي يتخفى بها هي

VBS Freelink

كيف تعرف أن هذا البرنامج موجود في جهازك وطريقة التخلص منه

أولا : قم بالبحث عن الملفات التالية

RUNDLL.VBS LINKS.VBS

و قد تحتاج هنا إلى تشغيل جهازك في الوضع الآمن لحذف هذه الملفات تماما

ثانيا : قم بإلغاء تلك الملفات من جميع السواقات التي على جهازك.

ثالثا : قم بحذف الجزء التالي من محرر التسجيل لديك عن طريق أبدأ ثم تشغيل ثم تكتب في المربع

Regedit

وستجد القيمة التالية فيه فقط قم بمسحها تماما

HKEY_LOCAL_MACHINESoftwaremicrosoftwindowsCurrentVersionRunRundll

RUNDLL.VBS=

بعد ذلك قم بأعادة تشغيل الويندوز

Happy99 :

وهو أيضا يضع خادم له داخل جهازك تحت اسم

SKA.EXE

وعند تنفيذه يظهر لك صندوق صغير يعرض به ألعاب نارية وأثناء عرض هذه الألعاب النارية يقوم بتحميل خادمة على جهازك دون أن تلاحظ ذلك.

ثم يقوم بتغير الملف

WSOCK32.DLL

ويحتفظ بالملف الأصلي تحت اسم

WSOCK32.SKA

ويقوم أيضا بوضع نفسه داخل سجل الويندوز ليتمكن من العمل كلما قمت بتشغيل جهازك. أيضا سوف يقوم بإرسال بريد ألكتروني إلى كل مستخدم أو شركة أخبار قمت بمراسلتهم مرفقا هذه الرسالة بالبرنامج نفسه

Happy99

وهذا واحد من البرامج القليلة التي تستطيع نشر نفسها بنفسها

الأسماء المستعارة لهذا البرنامج هي :

wsocks.ska ska.exe win32.ska ska

كيفية التخلص منة:

قم بالبحث عن الملفات التالية في المجلد التالي :

C:Windowssystem

SKA.DLL WSOCK32.SKA SKS.EXE

إذا وجدته فهو قد اخترق جهازك. قم مباشرة بإلغاء الملفات التالية :

SKA.DLL WSOCK32.DLL SKA.EXE

بعد ذلك قم بإعادة تسمية الملف

WSOCK32.SKA

إلى الاسم التالي

WSOCK32.DLL

K2Ps :

فقط يستطيع التمكن من وندوز 95 و وندوز 98 وقد انتشر عن طريق البريد الإلكتروني تحت اسم

K2PS.EXE

حيث تقول رسالة هذا البريد الذي قد يصل إلى أي شخص أن هناك فيروس اسمه

TX-500

وأنه هو برنامج مضاد لهذا الفيروس. طبعا كما تعرف هذه كانت مجرد كذبة ليتمكن من الدخول وسرقة معلومات اشتراكك مع مقدم خدمة الإنترنت بالإضافة إلى كلمة السر الخاصة بك ثم التحكم به وبالبريد الإلكتروني لك. وأيضا يمكنه تغيير كلمة السر الخاصة بك. والطريقة المفضلة إذا أحسست بهذا التغير قم مباشرة بتغير كلمة السر ثم قم بإلغاء الملفات التالية

K2PS.CFG K2PS.EXE

قم بتشغيل محرر التسجيل عن طريق أبدأ ثم تشغيل ثم أكتب

Regedit (شكل 1)

ثم أذهب إلى القيمة التالية وقم بمسحها

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowCurrentVersionC:
WINDOWSSYSTEMK2PS.EXE

Paradise :

وهو أقوى من برنامج

Back Orifice

ويحتاج أيضا إلى خادم يسمى

agent.exe

ويستطيع إلغاء ملفات وإنشائهم ويستطيع فتح وغلق النوافذ على جهازك

ويستطيع عمل محادثة معك

chatting

ويستطيع عمل أشياء أخرى.

كيفية التخلص منة :

يمكنك التخلص منة باستخدام البرنامج

The cleaner

وسوف تجد هذا البرنامج في الموقع التالي :

http://www.dynamsol.com/puppet/thecleaner.html

PrettyPrk :

هذا البرنامج يستطيع الانتشار أيضا عن طريق البريد الإلكتروني. فعند تنفيذه سوف يقوم بإرسال نفسه إلى العناوين الموجودة في

address book windows

وسوف يخبر المستخدمين الموجودين على IRC

عند إعدادات النظام وكلمات السر. وسوف يقوم بنسخ نفسه داخل المجلد التالي

C:WindowsSystem

مع الملف

files32.VXD

أيضا سوف يقوم بتسجيل نفسه داخل القيمة التالية في سجل الويندوز

HKEY_CLASSES_ROOT
exefileshellopencommandfiles32.vxd

فقط قم بإلغائها بالذهاب إلى أبدأ ثم تشغيل ثم أكتب

Rededit

: ProMail

انتشر كثيرا هذا البرنامج بطريقة

shareware و freeware

وقد انتشر تحت هذا الاسم

proml121.zip

وهو ملف غير مضغوط داخل هذا الملف

promail.exe

فإذا قمت بتحميلة على جهازك وقمت بعد تحميلة بالاشتراك مع أي شركة لخدمات البريد الإلكترونية فان جميع المعلومات التي أعطيتها لهذه الشركة إضافة إلى كلمة السر الخاصة بك يقوم هذا البرنامج بإرسالها إلى عنوان بريدي آخر غير معروف إي بطريقة عشوائية فكلما قمت بعملية اشتراك مع أي شركة أخرى لخدمات البريد الإلكتروني فان البرنامج يقوم بنفس العملية السابقة. :كيفية التخلص منة إذا كان لديك هذا البرنامج

Promail

قم مباشرة بإلغائه

: Sockets

وهذا البرنامج خطير جدا وهو تقريبا فيروس. وهو لا يقوم فقط بتحميل خادم له ولكنة يصيب عددا من الملفات المنتهية بالأحرف

exe

وله نفس خصائص البرامج الأخرى التي تعمل معالبريد الألكتروني والأيسكيو

كيفية التخلص منة : باستخدام البرنامج

Anti Troie

وهو برنامج جيد للقضاء علية وسوف تجده في الموقع التالي :

http://www.pobox.com/~cd

: ZipFile

وهو أيضا يتمكن من وندوز 95 و وندوز 98 و وندوز إن تي . وهو يستطيع نشر نفسه بنفسه باستخدام البريد الألكتروني

فإذا قمت بفتحة من بريدك الخاص فانه سوف يعرض الرسالة التالية :

file; it does not appear to be a valid archive. Cannot open set, insert the last disk of If this is part of a ZIP backup .help the backup set and try again. Please press F1 for

وعندما يتمكن من نشر نفسه باستخدام البريد الألكتروني فانه يقوم بإرسال نفسه مرة أخرى تحت اسم

Zipped_files.exe

إلى جميع العناوين التي استقبلت منهم رسائل سابقة مرفق به هذه الرسالة

received your email and I shall send you a Hi, username
this attached zip docs reply ASAP. Till then, take a look at
Bye

أيضا سوف يقوم هذا البرنامج بإلغاء جميع الملفات لديك والمنتهية بالأحرف التالية :

CPP H DOC XLS PPt C

وللأسف فأنة صعب جدا إن تستعيد تلك الملفات باستخدام الأمر undelete

الأسماء المستعارة لهذا البرنامج التي يتخفى تحتها هي :

worm.explore.zip win32.explore explore.zip

طريقة معرفة وجودة في جهازك والتخلص منه فقط لمستخدمي وندوز 95 و وندوز 98 قم بالضغط على

CTRL ALT DEL

وعند ظهور شاشة الإغلاق ولاحظت ظهور إحدى الملفات التالية فانه موجود في جهازك والملفات هي

Explore _setup Zipped_files

ملاحظة مهمة : يجب أن تفرق بين اسم الملف السابق

Explore

وبين المتصفح

Explorer

فإذا لاحظت إحدى الملفات السابقة فقم مباشرة بإلغاء الملفات التالية :

C:windows_setup.exe C:windowsExplore.exe

بعد ذلك قم بإلغاء الأسطر التالية والموجودة في

WIN.INI

باستخدام الأمر

msconfig او Sysedit

ثم اذهب إلى أبدأ ثم تشغيل والأسطر هي

run=c:windowssystemexplore.exe run=setup.exe

أيضا قم بإلغاء السطر التالي باستخدام الأمر

regedit

HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionWindowsRun

----

ما هي انواع الفايروسات ؟

النوع : bootSector

- الوصف :يقوم باستبدال الMBR عندما تبدأ جهازك يبدأ الفايروس بالعمل ثم يعمل الMbr و الذي وظيفته تحميل نظام التشغيل .هذا كان انجح أنواع الفايروسات حتى ظهور الماكرو
- مثال :Form
- الخطر : بسيط
- امكانية اكتشافه : سهل
- إزالته : سهل

النوع :TSR

- الوصف : عندما تشغيل برنامج مصاب يبدأ الفايروس بالعمل و يؤثر على كل البرامج التي تعمل في نفس الوقت.
- مثال :CaseCade
- الخطر : عالي
- الكشف: سهل
- الإزالة : ممكن احيانا

النوع : NON-Tsr أو File Viruse

- الوصف : عند تشغيل البرنامج المصاب فانه يبحث عن برامج أخرى للتأثير عليها و هو فايروس بطء و تأثيره بسيط لانه لا يبقى في الذاكرة و لا يتواجد عدد كبيرمن هذه النوعية.
- المثال: Vienna
- الخطر : عالي
- الكشف : سهل
- الازالة: سهله

النوع: Overwritin الناسخ

- الوصف: هذه الفايروسات تستبدل ملفات البرامج لديك و في النهاية لن تعمل البرامج لديك .و في اسوأ الحالات سيكون عليك إعادة تركيب البرنامج.
- مثال: Exterminator
- الخطر : بسط
- الكشف بسيط
- الازالة : بسيطة

النوع : MultiPartite

- النوع : هذا الفايروس خليط من الأنواع الثلاثة السابقة
- مثال: Tequilla
- الخطر : عالي
- الكشف : سهل
- الإزالة: ا حيانا يكون معقد .

النوع: Companion

- الوصف: هذا الفايروس يستغل الدوس و مزاياه .. فهو يبحث عن ملفات Com و EXE - ملفات تشغيل البرامج- عندما يعمل Com وتعمل الفايروسات عمل ExE و عند اتمام عملها تعمل EXE الحقيقية.و لهذا يصعب الوصل لها.
- مثال : aids
- الخطر : عالي
- الكشف: بسيط
- الازالة : بسيطة

النوع: Stealth

- الوصف : هذه النوعية مصممة لتصعب عملية العثور عليها من قبل البرامج المضادة للفايروسات.
- النوع:Frido
- الخطر : عالي
- الكشف: معقد
- الإزالة : سهل متى تم الكشف

النوع : Poly Morphic

- الوصف: البرامج المضادة للفايروسات تكشف عن الفايروسات عن طريق عمل مسح للنظام و البحث عن ما يسمى توقيع الفايروس و لكن هذه فايروسات ذكية جدا لا يمكن ان يظهر فيها نوعان من نفس الفصيلة بتوقيع واحد.
- مثال: Smeg
- الخطر : عالي
- الكشف : صعب

- الإزالة: صعبه

النوع : ماكرو

- الوصف :على عكس الانواع السابقة هذا كتب بلغة برمجية عالية HHL – قريبةمن اللغة الآدمية– و هي سهلة الكتابة و عالية الكفاءة في الشر طبعا .و هي يمكنها ان تصيب كل ملف جديدو في الغالب تستخدم نظام تلقائي لإرسال نفسها عن طريق البريد.
- مثال : Prilissa
- الخطر : عالي
- الكشف : قد يكون صعب أ حيانا
- الإزالة : سهل متىما تم التعرف عليه

النوع: Dropper

- الوصف: هو ليس فايروس بل تورجان يستخدم لتركيب الفايروس فيما بعد .
- مثال : Stoned Dropper

- الكشف : صعب جدا جدا
- الإزالة: سهله متى ماتم الكشف

النوع: Trojan تورجان

- الوصف: هي تنتقل لجهازك بينما انت تقوم بشئ آخر و هي من الممكن ان تدمر جهازك و تزعزع نظامك الامني و تجعلك عرضة للتجسس.
- مثال : Net Bus
- الكشف و الإزالة: سهل و مباشر

النوع: مزحة Joke

- الوصف :هي ليست فايروسات بل عبارة عن مزحة تخبرك ان فايروس تسلل لجهازك او ما شابه و هي آمنه و لا تشكل اي خطر على الاطلاق.
- مثال : Bonk

النوع : Hoax

- الوصف: عادة بريد الكتروني ينصحك بعدم فتح بريد معين او موقع معين و يطلب منك إرساله للجميع.
- مثال: Good Times

احذر من فيروس سيركوم .. مع طريقة التخلص منه

هل استلم احدكم في طيات بريدة الإلكتروني فحوى الرسالة التالية : ..Hi
?how are you
this file in order to get your opinion I send you
later. Thanks See you

سواء أكانت الإجابة بالإيجاب او النفي فليأخذ كل حذره

فإن وجدت رسالة تحمل نصا مثل هذا امسحها دون أن تفتحها فقد برز فيروس كمبيوتر جديد، بحيل جديدة، وخدع مبتكرة، يستطيع بها نشر نفسه من كمبيوتر إلى آخر مصطحبا معه بعض الملفات التي قد تحمل محتويات حساسة ويهاجم الفيروس الجديد أجهزة الكمبيوتر التي تعمل بنظام التشغيل ويندوز، ويخترق الملفات التي تحمل عناوين المراسلات، ومن ثم ينشر نفسه إلى ضحايا جدد، بعد أن يسرق وثائق عشوائية محملة على القرص الصلب كما يسعى الفيروس الجديد إلى إخفاء نفسه بتغيير النص الرئيسي في الرسالة التي يحملها، ويختار بالتالي عنوانا جديدا للرسالة في كل مرة ينتقل فيها وقد اكتشف الفيروس الجديد المعروف باسم الدودة أو وورم في منتصف يوليو/تموز الجاري، لكنه اكتسب قوته ببطء وبالتدريج زخم وتقول شركات مكافحة فيروسات الكمبيوتر إن الفيروس الجديد المسمي سيركام

يتزايد كفاءة، وإنه يصيب الآن أكثر عدد من الكمبيوترات منذ اكتشف في منتصف الشهر الحالي وتقول إحدى الشركات إنها رصدت حوالي أحد عشر ألفا وخمسمئة نسخة من سيركام في مئة وعشر دول، وأوقفت في الأربع والعشرين ساعة الأخيرة فقط أربعة آلاف نسخة وحذر متحدث باسم الشركة بأن أوروبا ستشعر بوطأة الفيروس قريبا وبينما اعتمدت فيروسات الحب والزوجة العارية وكورنيكوفا على السذاجة البشرية، وعلى ضعف برنامج ميكروسوفت أوت لوك الواسع الانتشار بين مستخدمي البريد الإلكتروني، يختلف الفيروس الجديد عن سابقيه بأنه يحمل في طياته برنامج البريد الخاص به، ولذلك يتنقل دون الاعتماد على معونة خارجية لكنه يتشابه مع الفيروسات السابقة في أن جهاز الكمبيوتر لا يصاب إلا بعد فتح الرسالة والملف الملحق بها خديعة وعلى النقيض من الفيروسات السابقة، يستطيع سيركام استلاب ملف العناوين في أي برنامج بريد إلكتروني يعمل على الويندوز، أو أي عناوين بريدية أخرى على متصفح الإنترنت المحمل على جهاز الكمبيوتر المصاب ويسرق سيركام أيضا ملفات عشوائية من على القرص الصلب ويلحقها بالرسائل التي يبعثها. وقد يتسبب هذا في إعاقة وسائط البريد الإلكتروني إذا كان حجم الملف الملحق كبيرا المصدر موقع البي بي سي على الرابطة أدناه :

http://news.bbc.co.uk/hi/arabic/news/newsid_1455000/1455821.stm

متابعة: Aims

سيمانتك تتطور أداة مجانية للتخلص من فيروس سيركوم

أنزلت سيمانتك المنتجة لعملاق مضاد الفيروسات الشهير نورتون أداة مجانية للتخلص الكلي من الفيروس العنقودي الجديد Sirc.com

والمعروف بالرسالة الترحيبية التي تقول مرحبا كيف حالكم hi how are you . ننصح جميع المشاركين هنا بأنزال هذة الأداة الجيدة اما مباشرة من موقع سيمانتك على الرابطة التالية : www.symantec.com او بالضغط على السطر الظاهر أدناه وهذة الأداة بريمج صغير حجمة لايتجاوز72 ك.ب ولكنة من القوة بمكان يؤهلك لقطع الشك باليقين إن كان هذا النوع من الفيروسات قد تشبث بجهازك ليتم القضاء علية تلقائيا.

الأخوان المستخدمين لنظام ويندوز ميلينيوم عليهم التقيد بتنفيذ الخطوات التي ستظهر لهم تلقائيا عند تنزيل الأداة على اجهزتهم وتفعليها Activating علما بأن هذة الأداة لاتحتاج الي عملية تحميل Installation حيث تعمل تلقائيا من خلال الريجيستري.

http://www.symantec.com/avcenter/FixSirc.com

تحذير من دودة (الشفرة الحمراء).. قد تضرب الأجهزة هذه الليلة !!

نبهت العديد من المواقع المتخصصة على شبكة الانترنت منذ صباح اليوم مستخدمي الكمبيوتر إلى اتخاذ إجراءات حماية من برنامج جديد ينتشر بسرعة كبيرة في أنحاء العالم.
إذ من المتوقع تقول هذه المصادر أن يقوم البرنامج الذي يعرف بـاسم (كود رد وورم) أي: دودة الشفرة الحمراء بغزو ملايين أجهزة الكومبيوتر، ابتداء من منتصف ليلة الثلاثاء حسب توقيت جرينتش.

وينصح مستخدمي الإنترنت بحماية أجهزتهم بواسطة تحميل رقعة خاصة من

موقع ميكروسوفت:

اضغط هنا

وكان فيروس آخر اسمه الدودة الحمراء قد غزا هذا الشهر نحو ربع مليون جهاز كومبيوتر في غضون تسع ساعات فقط.

وتستغل الدودة ثغرة في برامج تحميل خدمات الإنترنت التي تقدمها مايكروسوفت للأجهزة العاملة بنظام NT أربعة، وويندوز 2000، لكنها لا تؤثر على الأجهزة التي تستخدم برامج ويندوز 95، و98، والميلينيوم ME.

وتمحو الدودة الصفحة الرئيسية من المواقع الإنجليزية وتحل محلها عبارة "تم اختراقه عن طريق الصينيين". ويطلق لفظ دودة على الشفرة الحمراء، إذ لا يعتبر من الناحية التقنية فيروسا، لأن البرنامج يستطيع إصابة أجهزة كمبيوتر حتى دون أن يفعل مستخدمها خطأً ما.

وبسبب سرعة انتشار دودة الشفرة الحمراء، لم تتمكن شركات أمن الكمبيوتر من معرفة الشخص أو الجهة التي اخترعت البرنامج أو قامت بإطلاقه.

وأجبر هذا البرنامج وزارة الدفاع الأمريكية على غلق مواقعها في الفترة من العشرين حتى الرابع والعشرين من يوليو تموز.

ويذكر أن الهجوم يتم عن طريق إرسال أجهزة الكمبيوتر المصابة بالبرنامج عددا هائلا من الأوامر لدخول الموقع الأمر الذي يحول دون استجابة الموقع لهذه الأوامر .

خبير ينفي ان تكون الصين هي مصدر فيروس كود رد

ومن جهة اخرى نفى خبير صيني في فيروسات الكمبيوتر يوم الثلاثاء ان تكون الصين هي مصدر فيروس كود رد السريع الانتشار الذي اصاب مواقع للحكومة الامريكية على الانترنت الاسبوع الماضي رغم ان المواقع المعطلة ظهر عليها شعار يقول "اقتحمه صينيون".

فيروس كود رد قد يعود مرة أخرى !

حذرت الحكومة وخبراء تكنولوجيون من أن فيروس الكمبيوتر "كود رد" الذي أصاب 300 ألف جهاز كمبيوتر وعطل العديد من مواقع الحكومة الأمريكية على الإنترنت الأسبوع الماضي قد يعود للظهور من جديد بقوة أكبر.

وأفاد تقرير عن شركة مايكروسوفت ومركز حماية البنية الأساسية التابع لمكتب التحقيقات الاتحادي وجماعات أخرى صدر يوم الأحد أن الفيروس الذي ظهر لأول مرة يوم 19 يوليو/تموز الجاري من المتوقع أن يعود للظهور مساء يوم الثلاثاء ربما بشكل أكثر قوة.

وقامت تلك الجماعات ببحث أمر ذلك الفيروس في مؤتمر صحفي يوم الاثنين.

ويغزو الفيروس الذي اسماه المبرمجون كود رد على اسم مشروب خفيف أجهزة خادم الكمبيوتر ثم تصدر إليه الأوامر بان يغمر المواقع الحكومية بالمعلومات. وظهر على بعض المواقع المصابة شعارا يقول "اقتحمه صينيون."

وفي حين تمكن موقع البيت الأبيض من تجنب الأعطال يوم 19 يوليو/تموز الا ان وزارة الدفاع اوقفت الدخول على موقعها في 23 يوليو/تموز تحسبا للفيروس.

ويتوقع المسؤولون ان يؤدي الفيروس الذي أصاب 300 ألف جهاز كمبيوتر على الاقل الى ابطاء سرعة الانترنت بدرجة كبيرة عندما يعود للنشاط في الساعة الثامنة من مساء يوم الثلاثاء بتوقيت الساحل الشرقي للولايات المتحدة (0001 بتوقيت جرينتش يوم الاربعاء).

(مصادر متعددة)

كيف تلغي الفيروس آنا كورنيكوفا من جهاز الكمبيوتر؟

قبل يومين ضرب فيروس خطير أجهزة الكمبيوتر في أميركا الشمالية وأوروبا، أدى إلى تعطيل شركات خدمات البريد الإلكتروني.

يحمل الفيروس الذي ينتشر عبر البريد الإلكتروني اسم وصورة لاعبة التنس العالمية آنا كورنيكوفا، مما يغري مستخدمي البريد الالكتروني بفتح الرسائل لينتشر منها في الحال الفيروس.

وسرعان ما ينتشر الفيروس في كافة عناوين البريد الإلكتروني التي في حوزة المستخدم والموجودة في كتاب العناوين Address Book وكالعادة اختار مبرمج هذا الفيروس برنامج البريد الإلكتروني مايكروسوفت أوت لوك اكسبريس، لنشره الفيروس.

ولكن، كيف تتحرى وتتخلص من هذا الفيروس في حال ضرب جهازك؟

أولا :

قم بإجراء مسح لكمبيوترك Scan بواسطة برنامج مقاومة الفيروسات. استخدم >عيادة ماكافي< مثلا لهذا الغرض، فإذا كشفت العيادة وجود ملف يحمل الاسم VBS/SST@MM فقم بالخطوات التالية: اضغط بيمين الماوس فوقه ثم قم بإلغائه. بعد ذلك عليك القيام بإلغاء الإشارة والقيمة Value & Key من السجل Registry على الشكل التالي: أولا:

اختر Start/Run ثم أدخل الرمز regedit في خانة Open كما في الشكل رقم 1 ثم اضغط على Ok فتظهر نافذة السجل Registry كما هو مبين في الشكل رقم 2.

ثانيا: اضغط على علامة الزائد + الموجودة إلى يمين الملف HKEY_USERS

ثالثا: اضغط على علامة الزائد + الموجودة إلى يمين الملف DEFAULT.

رابعا: اضغط على علامة الزائد + الموجودة إلى يمين الملف SOFTWARE

خامسا: اضغط بيمين الماوس على الملف المسمى The Fly on وقم بإلغائه Delete وهكذا تخرج >آنا كورنيكوفا< من كمبيوترك الى الأبد.

ملاحظة: اسم ملف الفيروس آنا كورنيكوفا الذي قد يصلك بالبريد الالكتروني هو AnnaKournikova.jpg.vbs

خصائص الفيروسات:

1- القدرة على التخفي:

للفيروسات قدرة عجيبة على التخفي والخداع عن طريق الإرتباط ببرامج أخرى. كما تم أيضاً تزويد الفيروسات بخاصية التمويه والتشّبه. حيث أن

الفيروس يرتبط ببرنامج يقوم بأعمال لطيفة أو له قدرة عرض أشياء مثيرة، وعند بداية تشغيله يدخل إلى النظام ويعمل على تخريبه.

وللفيروسات عدة وسائل للتخفي منها ارتباطه بالبرامج المحببة إلى المستخدمين.. ومنها ما يدخل النظام على شكل ملفات مخفية بحيث لا تستطيع ملاحظة وجوده عن طريق عرض ملفات البرنامج.

وبعض الفيروسات تقوم بالتخفي في أماكن خاصة مثل ساعة الحاسب وتنتظر وقت التنفيذ.

كما أن بعضها تقوم بإخفاء أي أثر لها حتى أن بعض مضادات الفيروسات لا تستطيع ملاحظة وجودها ثم تقوم بنسخ نفسها إلى البرامج بخفة وسرية (تدري من أين تأكل الكتف) :).

2- الإنتشار:

يتميز الفيروس أيضاً بقدرة هائلة على الإنتشار. وقد سبق وأن قدمت العوامل التي تساعده في ذلك. [انظر الحلقة الثانية]

3- القدرة التدميرية:

تظهر عندما يجد الفيروس المفجر الذي يبعثه على العمل كأن يكون تاريخ معين (كفيروس تشرنوبل).

- أنواع الفيروسات:

1- فيروسات قطاع التشغيل (Boot Sector):

تصيب هذه الفيروسات قطاع التشغيل في القرص الصلب.. وهو الجزء الذي يقرؤه النظام عند كل مرة يتم فيها طلب تشغيل الجهاز.

2- فيروسات الملفات:

تلصق هذه الفيروسات نفسها مع ملفات البرامج التنفيذية مثل:
command.com أو win.com .

3- الفيروسات المتعددة الملفات:

تنسخ هذه الفيروسات نفسها في صيغة أولية ثم تتحول إلى صيغ أخرى لتصيب ملفات أخرى.

4- الفيروسات الخفية (الأشباح):

وهذه فيروسات مخادعة.. إذ أنها تختبئ في الذاكرة ثم تتصدى لطلب تشخيص وفحص قطاع التشغيل، ثم ترسل تقرير مزيف إلى السجل بأن القطاع غير مصاب.

5- الفيروسات متعددة القدرة التحوليّة:

وهذه الفيروسات لها القدرة الديناميكية على التحول وتغيير الشفرات عند الإنتقال من ملف إلى آخر، لكي يصعب اكتشافها.

6- فايروس المايكرو:

وهذا النوع من الفيروسات يختبئ في ملفات المايكرو للوورد. وتسمح تعليمات التهيئة المتطورة بأن تُنفّذ تلقائياً ضمن أي صيغة تختارها. كما يسمح "وورد بيسك" بالوصول المباشر لملفات النظام مما يجعل فيروس المايكرو قادراً على محو ملفات النظام أو حتى إعادة تهيئة النظام كاملاً (أو ما يعرف بعملية الفرمته).

بعد فيروس العاصفة :
دودة "سوبر وورم" تطل برأسها من جديد على أجهزة الكمبيوتر

يبدو أن مستخدمى الكمبيوتر أصبحوا فى الآونة الأخيرة على موعد دائم مع الفيروسات المدمرة التى ازدادت حدة هجماتها مع ظهور سلالة جديدة منها، بدءاً بثغرة مؤشر الماوس مروراً بفيروس العاصفة أو " storm 20 " الذى ضرب أكثر من 20 ألف جهاز وأخيراً ظهور أخطر أنواع الديدان الرقمية التي تغزو أجهزة الكمبيوتر وتتكاثر داخل ملفاته والتي تعرف باسم " سوبر وورم".

وأعلن باحثون في مجال فيروسات الكمبيوتر عن عودة هذا الفيروس والذى كان أول ظهور له في أكتوبر عام 2003 ويأتي فى شكل رسالة إما باللغة الانجليزية أو الالمانية، وتضم ملفا ملحقا بشفرة تخرب جهاز الكمبيوتر عند فتحها .

وأشار هون لاو كبير خبراء الامن الرقمي في شركة سيمانتك إلى أن الدودة القديمة قد أطلت برأسها مرة أخري علي ملفات الكمبيوتر ، وإنها تظهر علي شكل ملف يحمل اسم " W - 32 SUPER AA "، وقد بدأت في النشاط مجدداً يوم الاحد الماضي مشيرا إلي أن هذه الدودة تأتي في صورة رسالة بريد إلكتروني بنفس الاسم .

وتحتوى رسالة البريد الالكتروني التي تحمل هذا الفيروس فى طياتها عبارة " You told us that you forgot your password, we have to change the word for you For more details, please read the file on the password

Supplement"
أو "إنك أخبرتنا بأنك نسيت كلمة السر الخاصة بك وقد قمنا بتغيير هذه الكلمة من أجلك ولمزيد من التفاصيل برجاء قراءة الملف الملحق عن كلمة السر".

وبمجرد ضغط المستخدم علي الملف الملحق يقوم الفيروس بالانتشار داخل ملفات نظام الكمبيوتر، ويبدأ في التكاثر عند تشغيل البرامج، لذلك ننصح المستخدمين بتجنب مثل هذه الرسائل حرصا على عدم تعرض أجهزتهم للاختراق والتدمير

"العاصفة" يتضرب 20 ألف جهاز

وفي نفس الاتجاه، كشف المركز الدولي لرصد الفيروسات التابع لشركة سيمانتيك العالمية مؤخراً عن تجدد ظهور فيروس
" بصورة أكثر حدة عما كان عليه لدى storm"العاصفة" أو "
ظهوره لأول مرة خلال شهر يناير الماضي .

وذكرت مصادر داخل سيمانتك أن فيروس ستورم ضرب الحواسب بشدة خلال الأسبوع الماضي وأن المركز تلقى على الأقل نحو 20 ألف تقرير في يوم واحد يفيد تعرض حواسيب لاختراق من جانب هذا الفيروس الخبيث الذي تم تشفيرة لخداع برامج الحماية المنصوبة على تلك الأجهزة .

يُشار إلى أنه بمجرد إصابة جهاز المستخدم بهذا الفيروس فانه من المستحيل التخلص منه وإنقاذ برنامج التشغيل وبقية البرامج الأخرى الموضوعة على الجهاز بما يتعين معه إعادة تنصيب تلك البرامج مرة أخرى.

ولا يختفى هذا الفيروس داخل الرسالة العادية ولكنة يتخفى داخل ملف مضغوط في الرسالة ذاتها والتي تتكون من صورة وملف ، وتحتوى الصورة على كلمة المرور التى يتم بمقتضاها فتح الملف ، ولذلك يصعب على برامج الحماية التقليدية كشفه ومحاصرته وإيقافه.

وبالتالي فان المستخدم إذا أقدم على فتح الملف الذي يكون عنوانة "الحب" أو "تم رصد فيروس" أو غيرها من العبارات التى يستخدمها من قاموا بإنتاج هذة الدودة الضاره فان جهازه يتصل بشبكة متناظرة تقوم بسحب كافة ملفاته بما فيها الملفات الشخصية ثم تدمير البرامج بعد ذلك .

ويقوم الفيروس بعد ذلك بإعادة الجهاز المصاب إلى الحياة واستخدامة لإرسال رسائل ضارة محملة بالفيروس لكافة العناوين المسجلة على البريد الالكتروني لصاحب الجهاز، ويؤدى استخدام الدودة لشبكة متناظرة إلى استحالة السيطرة عليها حيث يتعين رصد كل حالة على حدة والتعامل معها بشكل منفرد .

فيروس مؤشر الماوس واستمرار مسلسل الاختراقات

بالرغم من إصدار شركة مايكروسوفت الأمريكية ملفاً لتحديث وسد ثغرة مؤشر الماوس التى ظهرت فى أنظمتها الشهر الماضي، أعلن مايك سكروبفر رئيس القسم الهندسي بشركة موزيلا لبرامج الكمبيوتر وصاحبة متصفح الإنترنت فاير فوكس أن متصفح الشركة فاير فوكس ليس محصنا ضد هذه الثغرة.

وأضاف سكروبفر أنه كان يوجد نوع من التشويش حول ما إذا كانت هذه الثغرة ستوجد أيضاً في متصفح فاير فوكس كما ظهرت في متصفح إكسبلورر لشركة مايكروسوفت في نظام ويندوز إلا أنه أكد أن هذه الثغرة موجودة أيضاً في فايرفوكس.

وأظهر أنه بالرغم من أن هذه الثغرة صعبة أمام القراصنة لاختراقها خلال متصفح فاير فوكس لأنه يعالج مؤشر الماوس بأشكاله الجديدة ويتعامل معه بشكل وبدرجة أقل من إكسبلورر إلا أن ذلك لا ينفي إمكانية اختراقها.

يأتي هذا في الوقت الذي أدي فيه تثبيت الملف الترقيعي patch الذي أصدرته مايكروسوفت الأسبوع الماضي لسد الثغرة الأمنية في أنظمة ويندوز التي استغلها مخترقو الأنظمة من خلال برنامج لتغيير شكل مؤشر الماوس، أدى إلى مشكلات لدى الكثير من المستخدمين .

فقد تبين أن الملف الترقيعي غير متوافق مع الأجهزة التي

تستخدم أنظمة سمعية وشبكية تصنعها شركة ريلتيك Realtek .

ومن جانبها، أكدت شركة مايكروسوفت وجود مشكلة في الملف الترقيعي، ووعدت بإصدار ملف ترقيعي جديد لحل هذه المشكلة الأسبوع القادم.

وتوجد هذه الثغرة الأمنية في تشغيل مؤشر الماوس فى كل أنظمة ويندوز بما في ذلك نظام فيستا الجديد، ويستطيع الهاكرز استغلال الثغرة للتسلل إلى الصفحات التي يدخلها المستخدم والدخول إلى بريده الإلكتروني ومعرفة بيانات سرية عنه.

بداية المشكلة
كانت مايكروسوفت قد أعلنت عن وجود ثغرة فى تشغيل مؤشر الماوس فى كل أنظمة ويندوز بما في ذلك نظام فيستا الجديد.

وتتيح هذه الثغرة للقراصنة التسلل إلى أجهزة الكومبيوتر التى يستخدم فيها المستخدمون مؤشر الماوس بأشكال متنوعة من خلال برامج لتغيير شكل الماوس.

وأظهرت مايكروسوفت أن القراصنة يمكنهم استغلال هذه الثغرة للتسلل إلى البريد الإلكترونى للمستخدم والدخول على صفحات شبكة الإنترنت ومعرفة بيانات سرية عنه.

(محمد اسماعيل محمد)
moonbook@live.com